



Release Note for the Cisco 11000 Series Secure Content Accelerator: SCA/SCA2

This release note applies to the Cisco 11000 Series Secure Content Accelerator, SCA and SCA2 versions. The note supplements information found in the *Cisco 11000 Series Secure Content Accelerator Configuration Guide* distributed with version 4.1 of the firmware. The SCA2 offers significantly higher performance than the other SCA device.

The Cisco 11000 Series Secure Content Accelerator is compatible with all Cisco content switches—the CSS 11500 and CSS 11000 Series Content Services Switches, the Cisco LocalDirector, and the Content Switching Module for the Catalyst 6500.

The following sections are presented in this note:

- CD Contents
- Reflashing the Firmware
- Operational Notes

CD Contents

The CD-ROM contains the following resources:

- Flash image
- Electronic versions of this document and the *Cisco 11000 Series Secure Content Accelerator Configuration Guide*

Reflashing the Firmware

The **fw** directory contains the firmware image of the SCA2. Use the following instructions to reflash the firmware on the device. Please read the entire document before proceeding with the flash procedure.

Serial Console CLI Instructions



Note

When flashing the SCA, use the file **css-sca-2fe-k9.phz**.

1. Copy the firmware image to an HTTP, FTP, or TFTP server on the same LAN as the Secure Content Accelerator. An FTP URL is preferable.
2. Connect to the Secure Content Accelerator via a serial management session at 9600 baud.
3. Enter these commands to load the firmware image, where *protocol* is HTTP, FTP, or TFTP; *serverip* is the IP address of the server; and *path* is the path to the firmware image file.)

```
enable
copy to flash protocol://serverip/path/css-sca2-2fe-k9.phz
reload
```

4. Wait for several minutes for the device to reload and reboot.
5. Check the firmware version by using the **show device** command. The returned text should contain "MaxOS 4.1".
6. Continue with configuration as desired.

Telnet CLI Instructions



Note

When flashing the SCA, use the file **css-sca-2fe-k9.phz**.

1. Copy the firmware image to an HTTP, FTP, or TFTP server on the same LAN as the Secure Content Accelerator. An FTP URL is preferable.
2. Connect to the Secure Content Accelerator using the IP address previously assigned to it.
3. Enter these commands to load the firmware image, where *protocol* is HTTP, FTP, or TFTP; *serverip* is the IP address of the server; and *path* is the path to the firmware image file.

```
enable
copy to flash protocol://serverip/path/css-sca2-2fe-k9.phz
reload
```

4. You will see a status message stating the connection to the device was lost. Wait for several minutes for the device to reload and reboot.
5. Reconnect to the device using a telnet management session.
6. Check the firmware version by using the **show device** command. The returned text should contain "MaxOS 4.1".
7. Continue with configuration as desired.

GUI Instructions



Note

When flashing the SCA, use the file **css-sca-2fe-k9.phz**.

1. Open a Web browser and connect to the Secure Content Accelerator.
2. Ensure that the **General>Status** page is displayed.
3. Click **Tools** to activate the Tools tabs.
4. Click the **Firmware** tab.
5. Type the path and firmware image file name or URL in the **Upload Firmware** text box, or click **Browse** and navigate to and select the firmware image file from the local file system.
6. Click **Upload** to load the firmware image into the GUI.
7. Click **Install Image** next to the file information in the **Installable Firmware Images** panel.
8. After the new firmware has uploaded, click the **Restart** tab.
9. Click **Reboot** to reload the device. Wait several minutes for the device to reboot.
10. Reconnect to the device using the GUI and the IP address assigned to it.
11. Click **General** to activate the General tabs.
12. The **Release** panel should contain “4.1”.
13. Continue with configuration as desired.

What's New in 4.1

- Configuration is no longer allowed from the remote configuration manager.
- Some TCP parameters can be configured using the TCP Tuning Configuration mode.
- A hybrid transparent mode (**transparent local-listen**) has been added.

Operational Notes

- To negotiate a connection with FIPS 104-2-compliant servers configured on the SCA2, some client browsers must be configured with TLS only. SSL must be disabled, and data is still encrypted.
- The commands **erase running-config** and **erase startup-config** are not available in FIPS Mode.
- The 4.x and previous versions of Netscape can “hang” when client authentication fails. If this happens, the server must be rebooted.
- If using IIS authentication, the basic form of Secure URL Rewrite cannot be used. The **redirectonly** option should be used.
- Configuring a device using multiple sessions or methods simultaneously can cause undesirable results. We recommend only one session be used at a time to make configuration changes.
- After changing a device from one-port to two-port mode (and vice versa), write the configuration to flash and reload (reboot) the device for proper functioning.

- Changing terminal settings in variance with the actual window size can affect the readline capabilities of the device: the displayed cursor position might not be indicative of its actual position.
- No error message is displayed when deleting an access list that is referenced by certain subsystems. Access is denied.

Network Design and Command Notes

- If your firewall or router filters traffic based upon MAC address, you must allow multiple MAC addresses per IP address on the interface connected to the device.
- Changing the interface speed and duplex from autonegotiation does not display forced configuration if open connections are present. Forced speed and duplex settings are displayed only if a non-autonegotiated speed is specified.
- Adding a static route entry for duplicating a previously RIP-discovered route is not supported.
- Deleting a RIP-discovered route is not supported.
- A RIP-discovered default route cannot be cleared with the command **clear ip routes** or by disabling RIP alone. To remove this type of route, disable RIP and reload the device.
- The command **ip route** does not allow a change to an existing entry. To change an entry, delete the old entry first and then add the new one.
- In two-port mode services such as syslog, RIP, RDATE server, SNTP server, and SNMP are available only through the “Server” port.
- Multiple subsystems can be set to use the same access port. However, this causes undesirable results. Please ensure each subsystem “listening” port is unique on the device.
- To use the syslog ability, the configured syslog server must be set to listen for remote entries.

Secure Server Notes

- Non-transparent server objects are not updated if the device IP address is changed. Reloading the device or accessing the configuration of each server object resets the IP address assignment.
- A saved configuration file does not contain private keys or passwords. Private keys must be loaded separately with names exactly matching those referenced by the secure server. Additionally, old private keys are not removed from the startup-configuration by copying a new configuration to the device. To remove the old private keys, delete each private key, and write the running-configuration to the startup configuration or erase the startup-configuration.
- When using client authentication, individual Web browsers behave very differently in the way they filter requests for client certificates and how they cache certain aspects of the session.

GUI Notes

- When setting up the device with SSL client-side GUI access, do not configure a non-transparent secure server to use the same localport.
- Erasing the running-configuration of a device using the GUI disconnects the Web browser from the device. To continue configuration, reconnect to the device.
- Setting the localport in a secure server entry to the listening TCP port of the Web management subsystem renders the GUI inaccessible. You must use a different listening TCP port for each entity.

- When writing a configuration via the GUI, the existing configuration is erased first; therefore, all configurations written using the GUI should be complete configurations. Incremental configuration updates are only possible by adding the changes to a complete configuration, and then writing this configuration. An option for overwriting or incrementally updating a configuration using a written configuration will be added at a future date.
- The GUI caches certain items and can misrepresent the state of the actual device in certain circumstances, such as if the device is rebooted without saving changes. To obtain the current device state, refresh the page. This can be accomplished by holding the SHIFT-clicking the **Refresh** button.
- Once Web management is enabled, it is always accessible via the “Server” port (two-port mode) or the “Network” port (one-port mode) even if SSL client-side access has been configured. Use an access list to prevent unwanted access.
- Assigning a Web management access list to the device completely prevents HTTPS access from the GUI. Setting the following access list allows HTTPS access to the GUI from any IP address:

```
access-list 10 permit 127.0.0.1 0.0.0.0
web-mgmt access-list 10
```

CLI Notes

- The **copy to startup-configuration** command replaces the public startup-configuration. The keys and passwords still exist unless they have been deleted or erased.
- Erasing the running-configuration of a device using the CLI disconnects any GUI or telnet sessions from the device. To continue configuration, reconnect to the device.
- The custom completer completes previously created objects with the word “create” if **TAB** is pressed after the full name is typed. To edit an existing object, ensure “create” is not part of the command.
- When writing configuration files to the running configuration, the new configuration file appends to the existing configuration rather than replacing it. In the process of recreating existing configuration information, some errors will be displayed. These can be ignored safely.

SNMP Notes

The factory-set default SNMP community is “public”; however, “public” is not listed in the configuration. The behavior of setting and resetting the SNMP community is demonstrated in the table below.

Command	SNMP community is set to...	SNMP community in configuration is...
snmp default community XYZ	XYZ	XYZ
no snmp default community	XYZ	No default community listed
snmp default community public	public	public

Windows NT 4.0-Specific Issues

- The arrow keys on the Windows NT 4.0 default telnet client when accessing the CLI do not behave as expected. To scroll through the command history, use **CTRL-N** and **CTRL-P**.
- Pasting certificates or keys using the default Windows NT telnet client may fail. This may be the result of the Return character at the end of each line in the file. If you open the file with Notepad and see black boxes at the end of each line, delete them and replace them with carriage returns using the **Enter** key. The file should load after this.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

Copyright © 2002, Cisco Systems, Inc.
All rights reserved.